LOAD BALANCING FOR A SYSTEM OF CRYPTOGRAPHIC PROCESSORS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application contains subject matter which is related to the subject matter of the following documents, each of which is assigned to the same assignee as this application. Each of the below listed documents is hereby incorporated herein by reference in its entirety:

[0002] Published U.S. Patent Application US 2006/0059373 A1 titled "Integrated circuit chip for encryption and decryption using instructions supplied through a secure interface" published Mar. 16, 2006;

[0003] U.S. Pat. No. 7,080,110 titled "Hardware implementation for modular multiplication using a plurality of almost entirely identical processor elements," issued Jul. 18, 2006.

[0004] U.S. patent application Ser. No. 11/331,918 titled "Methods for coordinating access to memory from at least two cryptography secure processing units" filed on Jan. 13, 2006.

[0005] The above referenced published patent application and issued patent are each members of two respective families of patent documents. The specifications of these documents are similar to the specifications of the other documents in their respective families.

TECHNICAL FIELD

[0006] This invention relates in general to controlling operations in a system of processor chips, and more particularly, to a method for controlling cryptographic processing operations presented in the form of a stream of request blocks. Even more particularly, the present invention is directed to a system and method which exploits the, secure, flexible and powerful capabilities of cryptographic processing chips which incorporate an internal cryptographic engine, a microprocessor and a field programmable gate array (FPGA) all of which exist behind a secure boundary. Although somewhat redundant in terms of the acronym used, these devices are referred to herein as COACH devices (Cryptography On A Chip) or COACH chips. The present invention exploits groups of these chips to more flexibly provide cryptographic processing, for encoding, decoding, signature verification and/or for authentication. Even more particularly the present invention exploits clusters of these groups of these chips and even further exploits internal cryptographic engines which support pipelined operations. The security features of these devices are discussed in the above referenced published patent application. These feature are not compromised in the practice of the present invention.

BACKGROUND OF THE INVENTION

[0007] In the patent referenced above there is disclosed a circuit for performing multiplication modulo N, where N is preferably a large prime number. Such circuits are useful for carrying out exponentiation operations modulo N. Such mathematical operations lie at the heart of a significant number of methods for encrypting and for decrypting data. The circuits disclosed provide a powerful and flexible method for such processing using concatenated arrays of what are referred to therein as "processing elements." The similarity in structure of these processing elements is also seen to be of value in structuring a process in which operations are pipelined, thus increasing overall throughput. Accordingly, it is seen that the referenced issued patent provides a useful cryptographic engine which is used in the present invention.

[0008] It is also seen that the above referenced published patent application discloses a secure processing chip which includes: a cryptographic engine such as the one in the above-mentioned issued patent, a microprocessor, an internal memory, and a hybrid FPGA/ASIC (Application Specific Integrated Circuit) chip controller. This controller provides a secure mechanism along with internal hardwired cryptographic key structures, such as fuses, which are used in decoding instruction streams which are passed to chip internals as a method for providing secure programming and structure for the FPGA/ASIC chip controller. In their normal operation subsequent to secure programming operations, these processing chips (COACH devices) receive strings of instructions through an I/O interface in the form of request blocks which may or may not be encrypted.

[0009] These chips are useable in groups without impacting their secure nature. An array of these groups is employed in the present invention. This structure provides a more flexible system which is capable of cryptographic processing in which the length of the keys is employable as a selector of the number of COACH chips to be employed in a given encryption or decryption operation or string of operations.

SUMMARY OF THE INVENTION

[0010] The shortcomings of the prior art are overcome and additional advantages are provided through the use of a system and method for controlling cryptographic operations in a plurality of cryptographic processors. The method comprises three basic steps. The first is the provision of a plurality of instruction streams from a system memory. The second is the step of supplying these instruction streams to the processors based initially on addresses within the memory. In the third step, subsequent instruction streams are retrieved by a controller from the memory based on a dynamic partitioning of the locations within the memory.

[0011] In accordance with one embodiment of the present invention, the instruction streams are supplied to the processors in a manner which takes advantage of the fact that the cryptographic engines within the processor elements are operable in a pipelined fashion. In this manner, cryptographic operations that are preferably carried out in a serial fashion may be so processed while at the same time cryptographic operations that are preferably processed in a parallel fashion may likewise be processed in this manner. In short, the structure of the processor elements **100**, either within a group or within an array of groups is such as to provide processing flexibility.

[0012] Accordingly, it is seen that it is an object of the present invention to improve the operations of cryptographic devices for encoding, decoding, signature verification and authentication.

[0013] It is also an object of the present invention to exploit the pipelined structure present in some cryptographic engines.

[0014] It is yet another object of the present invention to provide load balancing to an array of cryptographic processors to thus produce an increase in performance.